Cryptojacking incidents in the UK rose by 1,200% in last few months

1 March 2018 | Author: Jay Jay

The UK saw cryptojacking attacks rise by 1,200 percent in the past few months, making it among the top five countries in the world in terms of the number of such attacks.

Cyber criminals are increasingly mining cryptocurrency using covert means like exploiting processing power of victims' systems without informing them about such activities.

The UK today ranks fourth in the world in terms of cryptojacking attacks thanks to a sudden rise in the number of such attacks in the past six months, Symantec Threat Intelligence has revealed. As of now, only the United States, Japan, and France face more cryptojacking attacks compared the UK.

The firm revealed that in the past few months, incidents of cryptojacking, that involves hackers using the processing power of victims' systems to mine cryptocurrency, rose by 1,200 percent in the UK, thereby revealed how widespread the entire operation is. In the past few months, Britain accounted for 4 percent of all cryptojacking incidents that took place around the world.

In February, a massive cryptocurrency mining operation (https://teiss.co.uk/threats/cryptocurrency-mining-operation/) forced the government to shut down hundreds of websites belonging to the Student Loans Company, several NHS services, and

RECOMMENDED


(https://teiss.co.uk
ministries-
network-hacked/?
getcat=)


(https://teiss.co.uk
cyber-attacks-
post-brexit/?
getcat=)

local councils. The operation was carried out by hackers who compromised a widely-used browser plug-in to spread their web to thousands of websites and subsequently mined cryptocurrency using the processing power of infected devices.

After the operation was discovered and urgent steps were taken to limit its spread, Andrew Douthwaite, VP Managed Services at VirtualArmour, told *Express.co.uk* that the cryptojacking operation could be the first of many such operations to take place in the UK.

“This method of thinking around how effective a ‘hack’ or ’attack’ is becoming more common, we are not seeing individual sites or companies being targeted, but common services, or ancillary third party plugins being targeted.

“This gives the attackers a much wider audience to hit at once, the third party companies developing the add-ons or additional services are generally smaller than the companies using them and therefore can be less stringent with their QA and security. Another example of this approach was the huge DDoS attack on the DNS provider Dyn – taking down, Twitter Netflix, Spotify to name but a few,” he said.

Despite a rapid increase in cryptojacking incidents, researchers believe such efforts aren't as destructive as ransomware injections or phishing scams as hackers do not steal credentials or inject powerful malware into victims' systems.

"The in-browser cryptocurrency miners are not installing anything on the victim's machines, they're not encrypting files. Even though they could potentially steal credentials, at the moment the attackers don't want to," Candid Wueest, a researcher at Symantec, told *Sky News* (https://news.sky.com/story/cryptojacking-attacks-surge-1200-in-uk-11269594).

However, Steve Giguere, lead EMEA engineer at Synopsys, has warned that the technique that hackers employed last month to use government websites to mine cryptocurrency, could also be employed for DDoS attacks in the future.

"As hackers are always looking for a weak link, we can expect browser plug-ins will continue to be an active target to exploit the distributed horse-power of browser based computing. In this particular incident, a plug-in which would be used by organisations who have a large user base and have demonstrated in the past (WannaCry) a potential to be an easy target, no doubt incentivised the attackers," he said.

RELATED ARTICLES

- Communications network used by several ministries was hacked, Germany confirms (https://teiss.co.uk/threats/germany-ministries-network-hacked/?getcat=)
- Brexit could impact the UK’s ability to deter cyber attacks, experts warn (https://teiss.co.uk/threats/uk-cyber-attacks-post-brexit/?getcat=)
- Critical infrastructure organisations are prime targets for hackers, says Anomali (https://teiss.co.uk/threats/critical-infrastructure-organisations-hackers/?getcat=)
- UK-based think tanks frequently targeted by Chinese hackers in 2017 (https://teiss.co.uk/threats/uk-think-tanks-chinese-hackers/?getcat=)
- CCTV cameras at British schools hacked & their live feeds broadcasted on US website (https://teiss.co.uk/threats/cctv-cameras-british-schools-hacked/?getcat=)

Bio | Latest Posts

Jay Jay

Jay has been a technology reporter for almost a decade. When not writing about cybersecurity, he writes about mobile technology for the likes of Indian Express, TechRadar India and Android Headlines

(http://twitter.com/Jayjay_tech)

(https://www.facebook.com/profile.php?id=100009407656255&ref=bookmarks)

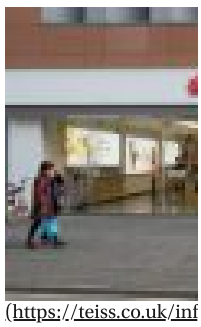
(https://plus.google.com/114154621250737298038?rel=author)

(https://teiss.co.uk/infrastructure-organisations-hackers/?getcat=)

(https://teiss.co.uk/think-tanks-chinese-hackers/?getcat=)

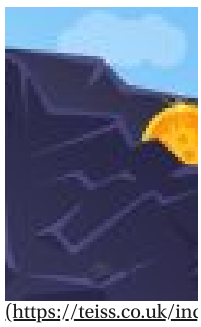
(https://teiss.co.uk/cameras-british-schools-hacked/?getcat=)

MOST POPULAR



(https://teiss.co.uk/inf
security/huawei-uk-nc
INFORMATION SECURITY (/CA
SECURITY)

Despite U.S. ban, Huav
from UK's NCSC
(https://teiss.co.uk/inf
security/huawei-uk-nc



(https://teiss.co.uk/inc
miners-future-cyber-d
INDUSTRY VIEW (/CATEGORY

Crypto-Miners and the
(https://teiss.co.uk/inc
miners-future-cyber-d

Comments

0 Comments Sort by Newest

Add a comment...

Facebook Comments Plugin

Tags: cryptocurrency (https://teiss.co.uk/tag/cryptocurrency/), Cyber threat (https://teiss.co.uk/tag/cyber-threat/), Information Security (https://teiss.co.uk/tag/information-security-2/), mining (https://teiss.co.uk/tag/mining-2/)

RELATED ARTICLES

(https://teiss.co.uk/threats/germany-ministries-network-hacked/)

THREATS (HTTPS://TEISS.CO.UK/CATEGORY/THREATS/)

Communications network used by several ministries was hacked, Germany confirms (https://teiss.co.uk/threats/germany-ministries-network-hacked/)

(https://teiss.co.uk/threats/uk-cyber-attacks-post-brexit/)

THREATS (HTTPS://TEISS.CO.UK/CATEGORY/THREATS/)

Brexit could impact the UK's ability to deter cyber attacks, experts warn (https://teiss.co.uk/threats/uk-cyber-attacks-post-brexit/)

(https://teiss.co.uk/threats/critical-infrastructure-organisations-hackers/)

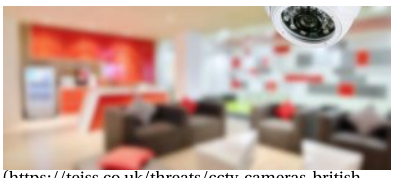
THREATS (HTTPS://TEISS.CO.UK/CATEGORY/THREATS/)

Critical infrastructure organisations are prime targets for hackers, says Anomali (https://teiss.co.uk/threats/critical-infrastructure-organisations-hackers/)

(https://teiss.co.uk/threats/uk-think-tanks-chinese-hackers/)

THREATS (HTTPS://TEISS.CO.UK/CATEGORY/THREATS/)

UK-based think tanks frequently targeted by Chinese hackers in 2017 (https://teiss.co.uk/threats/uk-think-tanks-chinese-hackers/)



(https://teiss.co.uk/threats/cctv-cameras-british-schools-hacked/)

THREATS (HTTPS://TEISS.CO.UK/CATEGORY/THREATS/)

CCTV cameras at British schools hacked & their live feeds broadcasted on US website (https://teiss.co.uk/threats/cctv-cameras-british-schools-hacked/)

(https://teiss.co.uk/threats/iot-devices-cyber-attacks-interpol/)

THREATS (HTTPS://TEISS.CO.UK/CATEGORY/THREATS/)

All IoT devices are potentially at risk of cyber attacks, warns Interpol (https://teiss.co.uk/threats/iot-devices-cyber-attacks-interpol/)

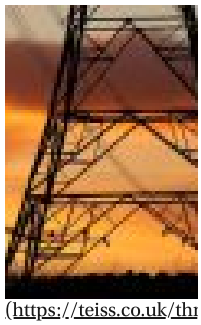
SHOW MORE LIKE THIS (HTTPS://TEISS.CO.UK/CATEGORY/THREATS/?MORE=LIKETHIS)

(https://teiss.co.uk/ne
campaign/)
NEWS (/CATEGORY/NEWS)

Malicious email campa
banking trojan unearth
(https://teiss.co.uk/ne
campaign/)

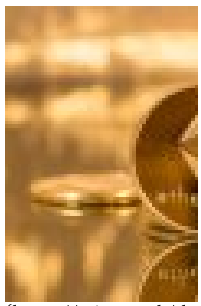
(https://teiss.co.uk/ne
cleansing-gdpr/)
NEWS (/CATEGORY/NEWS)

One-third of UK organi
data-cleansing process
(https://teiss.co.uk/ne
cleansing-gdpr/)



(https://teiss.co.uk/thr
ukrainian-power-outag
NEWS (/CATEGORY/NEWS) / T

Malware attacks behin
outage, researchers rev
(https://teiss.co.uk/thr
ukrainian-power-outag



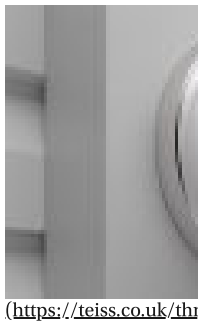
(https://teiss.co.uk/thr
hacks-hacking-unhack
accounts/)
FEATURES (/CATEGORY/FEAT
/ OPINION (/CATEGORY/OPIN
(/CATEGORY/THREATS)

Crypto currency hacks
(https://teiss.co.uk/thr
hacks-hacking-unhack
accounts/)

(https://teiss.co.uk/iot
risk-by-failing-to-prote
accounts/)

IOT (/CATEGORY/IOT) / THREA

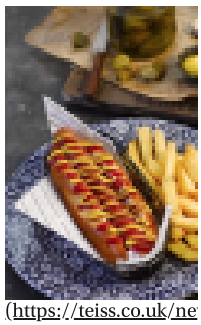
Leaders putting firms a
social media accounts
(https://teiss.co.uk/iot
risk-by-failing-to-prote
accounts/)



(https://teiss.co.uk/thr
meters-security-gchq/

THREATS (/CATEGORY/THREA

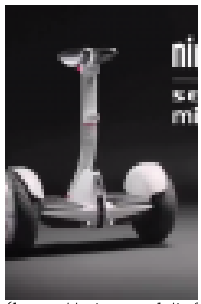
Poorly-secured smart e
millions at risk from ha
(https://teiss.co.uk/thr
meters-security-gchq/



(https://teiss.co.uk/ne
customer-data-gdpr/)

INFORMATION SECURITY (/CA
SECURITY) / NEWS (/CATEGO

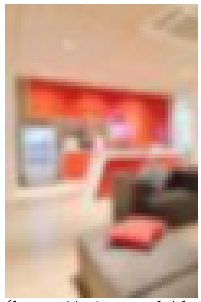
Did Wetherspoons del
fear of GDPR's immine
(https://teiss.co.uk/ne
customer-data-gdpr/)



(https://teiss.co.uk/inf
flaws-segway-hoverboa

INFORMATION SECURITY (/CA
SECURITY) / NEWS (/CATEGO

Critical flaws in Segwa
them vulnerable to cyb
(https://teiss.co.uk/inf
flaws-segway-hoverboa



(https://teiss.co.uk/thr
schools-hacked/)

THREATS (/CATEGORY/THREA

CCTV cameras at Britis
live feeds broadcasted
(https://teiss.co.uk/thr
schools-hacked/)

(https://teiss.co.uk/ne
government-websites/

NEWS (/CATEGORY/NEWS)

Anonymous takes dow
websites to support Ca
(https://teiss.co.uk/ne
government-websites/

(https://teiss.co.uk/ne
university-personal-de

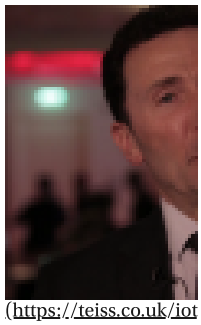
HUMAN FACTORS (/CATEGOR
INFORMATION SECURITY (/CA
SECURITY) / NEWS (/CATEGO

Data breach at Univers
students' personal deta
(https://teiss.co.uk/ne
university-personal-de

(https://teiss.co.uk/inf
small-businesses-read

INFORMATION SECURITY (/CA
SECURITY)

Only 10% of small busi
finds FSB (https://teiss
security/10-small-busi
fsb/)



(https://teiss.co.uk/iot
future-cyber-security-r
IOT (/CATEGORY/IOT) / VIDEO

How the LSE prepares
regulations (https://tei
prepares-for-future-cy

(https://teiss.co.uk)

Home (https://teiss.co.uk/)
Current Affairs (https://teiss.co.uk/category/current-affairs/)
Legislation/GDPR (https://teiss.co.uk/category/legislation/)
Threats (https://teiss.co.uk/category/threats/)
IoT (https://teiss.co.uk/category/iot/)
Culture (https://teiss.co.uk/category/business-culture/)
Process (https://teiss.co.uk/category/process/)
Features (https://teiss.co.uk/category/features/)
Glossary (https://teiss.co.uk/glossary/glossary-a/)
Video (https://teiss.co.uk/category/video/)

Video campaigns (http://www.lyonsdown.co.uk/publications/prosi
MediaKit.pdf)
Telegraph microsites (http://www.lyonsdown.co.uk/publications/prosi
Breakfast briefings (http://media-kits.business-reporter.co.uk/breakfast-briefings/)
Online Partnerships (http://media-kits.business-reporter.co.uk/teiss-partnership)
Testimonials (https://teiss.co.uk/testimonial/)
Subscribe to our newsletters (https://marketing.teiss.co.uk/acton/media/3199
--sign-up-to-our-newsletter)
Terms of Use (https://teiss.co.uk/privacy/)
Privacy (https://teiss.co.uk/privacy-2/)
About Teiss.co.uk (https://teiss.co.uk/about-teiss-co-uk/)
Contact Us (https://teiss.co.uk/contact-us/)

23-29 He
London,

020 8349

press@te
(mailto:p